

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended): A method for securing an accessible computer system, the method comprising:

monitoring for connection transactions between multiple access requestors and an access providers provider at a switch that is connected to the access ~~providers~~ provider and that transfers data to and from the access ~~providers~~ provider;

~~based on the monitoring, determining, by the switch, whether a cumulative number of connection transactions initiated to more than one of the access providers by an attacking access requestor during a first period of time exceeds a threshold number; and~~

when the monitoring reveals that one of the multiple access requestors is an attacking access requestor, denying, at the switch, access by the attacking access requestor to the access providers provider for a time out period during which the attacking access requestor is denied access to the access provider; and ~~in response to a determination that the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor exceeds the threshold number during the first period of time~~

in response to detecting a new connection transaction initiated by the attacking access requestor during the time out period, starting a new time out period and continuing to deny access by the attacking access requestor during the new time out period.

2. (Canceled)

3. (Currently Amended): The method as in claim [[1]] 59, wherein the monitoring further includes counting, using the switch, the number of connection transactions initiated by the access requestors to any of the access providers through the switch during the first period of time.

4. (Currently Amended): The method as in claim [[1]] 59, wherein:
the determining further includes comparing, using the switch, the number of connection transactions initiated by the access requestors through the switch during the first period of time to the threshold number.

5. (Canceled)

6. (Currently Amended): The method as in claim [[1]] 59, wherein the monitoring further includes counting, using the switch, the cumulative number of connection transactions initiated to any of the access providers by the attacking access requestor during the first period of time such that the cumulative number of connection transactions reflects connection transactions initiated to all of the access providers by the attacking access requestor.

7. (Previously Presented): The method as in claim 6, wherein the determining further includes comparing, using the switch, the cumulative number of connection transactions initiated by the attacking access requestor during the first period of time to the threshold number, and
denying access by the attacking access requestor to the access providers includes denying, using the switch, access by the attacking access requestor to all of the access providers connected to the switch when the comparison results indicate that the cumulative number of connection transactions initiated by the attacking access requestor during the first period of time exceeds the threshold number.

8. (Original): The method as in claim 6, wherein the monitoring includes monitoring a computer system for connection transactions made using TCP.

9. (Previously Presented): The method as in claim 46, wherein the detecting includes identifying the Internet protocol addresses through the use of a header attached to a message representing a connection transaction being detected.

10. (Currently Amended): The method as in claim 1, wherein the denying of access includes denying access to the access ~~providers~~ provider through the switch by the attacking access requestor for a second configurable period of time.

11. (Cancelled)

12. (Currently Amended): The method as in claim 1, wherein the denying of access includes denying access to the access ~~providers~~ provider through the switch by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the attacking access requestor through the switch.

13. (Currently Amended): The method as in claim 1, wherein the access requestors are clients and the access ~~providers are hosts~~ provider is a host such that the monitoring includes detecting connection transactions through the switch between multiple clients and the host ~~multiple hosts~~.

14. (Previously Presented): The method as in claim 3, wherein the counting further comprises counting, using the switch, a cumulative number of connection transactions for all of the access providers connected to the switch initiated by each of the access requestors during the first period of time.

15-24. (Cancelled)

25. (Currently Amended): A system for securing an accessible computer system, comprising:

a switch that is connected to an access providers provider and that includes at least one hardware component configured to:

monitor for connection transactions between multiple access requestors and the access providers provider;

~~based on the monitoring, determine whether a cumulative number of connection transactions initiated to more than one of the access providers by an attacking access requestor during a first period of time exceeds a threshold number; and~~

when the monitoring reveals that one of the multiple access requestors is an attacking access requestor, deny, at the switch, access by the attacking access requestor to the access providers provider for a time out period during which the attacking access requestor is denied access to the access provider; and in response to a determination that the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor exceeds the threshold number during the first period of time

in response to detecting a new connection transaction initiated by the attacking access requestor during the time out period, start a new time out period and continue to deny access by the attacking access requestor during the new time out period.

26. (Currently Amended): The system of claim [[25]] 61, wherein the switch comprises: a detection component that is structured and arranged to detect connection transactions initiated by the access requestors through the switch;

a counting component that is structured and arranged to count the number of connection transactions initiated by the access requestors to any of the access providers through the switch during the first period of time;

a comparing component that is structured and arranged to compare the number of connection transactions initiated by the access requestors through the switch during the first period of time to the threshold number; and

the switch is configured to deny access by the attacking access requestor to all of the access providers when the comparison results indicate that the number of connection transactions

initiated by the attacking access requestor during the first period of time exceeds the threshold number.

27. (Currently Amended): The system of claim ~~[[25]]~~ 61, wherein the switch comprises:
a counting component that is structured and arranged to count the cumulative number of connection transactions to any of the access providers initiated through the switch by the attacking access requestor during the first period of time such that the cumulative number of connection transactions reflects connection transactions initiated to all of the access providers by the attacking access requestor;

a comparing component that is structured and arranged to compare the cumulative number of connection transactions initiated through the switch by the attacking access requestor during the first period of time to the threshold number; and

the switch is configured to deny access by the attacking access requestor to all of the access providers when the comparison results indicate that the cumulative number of connection transactions initiated by the attacking access requestor during the first period of time exceeds the threshold number.

28. (Original): The system of claim 27, wherein the connection transactions include connections made using TCP.

29. (Previously Presented): The system of claim 27, further comprising:
an identifying component that is structured and arranged to identify Internet protocol addresses through the use of a header attached to a message representing a connection transaction being detected.

30. (Currently Amended): The system of claim 25, wherein the switch comprises:

an access preventer that is structured and arranged to deny access to the access ~~providers~~ provider through the switch by the attacking access requestor for a second configurable period of time.

31. (Currently Amended): The system of claim 30, wherein the switch further comprises:
a timing component that is structured and arranged to measure the second configurable period of time during which the access preventer denies access to the access ~~providers~~ provider by the attacking access requestor.

32. (Cancelled)

33. (Currently Amended): The system of claim 25, wherein the switch comprises:
an access preventer that is structured and arranged to deny access to the access ~~providers~~ provider through the switch by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the access requestor.

34. (Currently Amended): The system of claim 25, wherein the access requestors are clients and the access ~~providers are hosts~~ provider is a host such that the switch comprises:
a detection component that is structured and arranged to detect connection transactions through the switch between multiple clients and the host ~~multiple hosts~~.

35. (Previously Presented): The system of claim 26, wherein the counting component further comprises counting a cumulative number of connection transactions for all of the access providers connected to the switch initiated by each of the access requestors during the first period of time.

36. (Previously presented): The system of claim 25, wherein a host computer system receives communications from the switch.

37. (Previously presented): The system of claim 25, wherein the switch is included in a host computer system.

38. (Currently Amended): The method of claim [[1]] 59 wherein denying access by the attacking access requestor to the access providers comprises denying, using the switch, access by the attacking access requestor to all of the access providers connected to the switch irrespective of which of the access providers to which the attacking access requestor initiated connection transactions to exceed the threshold.

39. (Currently Amended): The method of claim [[1]] 59 wherein the monitoring includes monitoring, using a switch configured to establish communication links between access requestors and access providers, for attempts, by the attacking access requestor, to establish a communication link with any of the access providers.

40. (Previously Presented): The method of claim 39 wherein monitoring for attempts, by the attacking access requestor, to establish a communication link with any of the access providers includes monitoring for attempts, by the attacking access requestor, to establish a communication link with any of the access providers, the establishment of a communication link between the attacking access requestor and one of the access providers involving exchange of more than two electronic messages.

41-44. (Cancelled)

45. (Currently Amended) The method of claim [[1]] 59 wherein:
the access providers include a first access provider and a second access provider that is different from the first access provider, and

the monitoring takes into account interactions of the attacking access requestor with both the first access provider and second access provider.

46. (Currently Amended) The method of claim [[1]] 59 wherein the monitoring includes detecting connection transactions between multiple Internet protocol addresses and the access providers with the switch.

47. (Currently Amended) The method of claim [[1]] 59 wherein determining, by the switch, whether the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during the first period of time exceeds the threshold number comprises determining, by the switch, whether a cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during a first configurable period of time exceeds a configurable threshold number.

48. (Currently Amended) The method of claim [[1]] 59 wherein determining, by the switch, whether the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during the first period of time exceeds the threshold number comprises determining, by the switch, whether a total number of connection transactions initiated to all of the access providers by the attacking access requestor during the first period of time exceeds the threshold number.

49. (Currently Amended) The method of claim [[1]] 59 wherein determining, by the switch, whether the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during the first period of time exceeds the threshold number comprises determining that the cumulative number of connection transactions exceeds the threshold number despite a number of connection transaction initiated to each of the more than one of the access providers individually being less than the threshold number.

50. (Currently Amended) A switch comprising:
a processor; and

a memory encoded with machine readable instructions that, when executed by the processor, operate to cause the processor to perform operations comprising:

transferring data to and from an access providers provider;

monitoring, at the switch, for connection transactions between multiple access requestors and the access providers provider;

~~based on the monitoring, determining, by the switch, whether a cumulative number of connection transactions initiated to more than one of the access providers by an attacking access requestor during a first period of time exceeds a threshold number;~~
and

when the monitoring reveals that one of the multiple access requestors is an attacking access requestor, denying, at the switch, access by the attacking access requestor to the access providers provider for a time out period during which the attacking access requestor is denied access to the access provider; and in response to a determination that the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor exceeds the threshold number during the first period of time

in response to detecting a new connection transaction initiated by the attacking access requestor during the time out period, starting a new time out period and continuing to deny access by the attacking access requestor during the new time out period.

51. (Currently Amended) The switch of claim ~~[[50]]~~ 62, wherein the monitoring further includes counting, using the switch, the cumulative number of connection transactions initiated to any of the access providers by the attacking access requestor during the first period of time such that the cumulative number of connection transactions reflects connection transactions initiated to all of the access providers by the attacking access requestor.

52. (Previously Presented) The switch of claim 51, wherein the determining further includes comparing, using the switch, the cumulative number of connection transactions initiated by the attacking access requestor during the first period of time to the threshold number, and

denying access by the attacking access requestor to the access providers includes denying, using the switch, access by the attacking access requestor to all of the access providers connected to the switch when the comparison results indicate that the cumulative number of connection transactions initiated by the attacking access requestor during the first period of time exceeds the threshold number.

53. (Currently Amended) The switch of claim 50, wherein the denying of access includes denying access to the access ~~providers~~ provider through the switch by the attacking access requestor for a second configurable period of time.

54. (Cancelled)

55. (Currently Amended) The switch of claim ~~[[50]]~~ 62 wherein the monitoring includes detecting connection transactions between multiple Internet protocol addresses and the access providers with the switch.

56. (Currently Amended) The switch of claim ~~[[50]]~~ 62 wherein determining, by the switch, whether the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during the first period of time exceeds the threshold number comprises determining, by the switch, whether a cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during a first configurable period of time exceeds a configurable threshold number.

57. (Currently Amended) The switch of claim ~~[[50]]~~ 62 wherein determining, by the switch, whether the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during the first period of time exceeds the threshold number comprises determining, by the switch, whether a total number of connection transactions initiated to all of the access providers by the attacking access requestor during the first period of time exceeds the threshold number.

58. (Currently Amended) The switch of claim [[50]] 62 wherein determining, by the switch, whether the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during the first period of time exceeds the threshold number comprises determining that the cumulative number of connection transactions exceeds the threshold number despite a number of connection transaction initiated to each of the more than one of the access providers individually being less than the threshold number.

59. (New) The method of claim 1 wherein the monitoring comprises monitoring for connection transactions between multiple access requestors and access providers at a switch that is connected to the access providers and that transfers data to and from the access providers, further comprising:

based on the monitoring, determining, by the switch, whether a cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during a first period of time exceeds a threshold number.

60. (New) The method of claim 1 wherein starting the new time out period and continuing to deny access by the attacking access requestor during the new time out period comprises resetting a timer that is measuring the time out period during which the attacking access requestor is denied access to the access provider.

61. (New) The system of claim 25 wherein the at least one hardware component is configured to monitor for connection transactions between multiple access requestors and access providers and, based on the monitoring, determine whether a cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during a first period of time exceeds a threshold number.

62. (New) The switch of claim 50 wherein the monitoring comprises monitoring for connection transactions between multiple access requestors and access providers and the operations further comprise, based on the monitoring, determining, by the switch, whether a

Applicant : Joseph Barrett et al.
Serial No. : 09/666,140
Filed : September 20, 2000
Page : 13 of 16

Attorney's Docket No.: 24838-0003001 / Security 08

cumulative number of connection transactions initiated to more than one of the access providers
by the attacking access requestor during a first period of time exceeds a threshold number.